

CERTIFICATE OF MAILING BY EXPRESS MAIL

"EXPRESS MAIL" Mailing Label No. EL063369769US

Date of Deposit: January 15, 1999

I hereby certify that this paper or fee is being deposited with the U.S. Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Box Patent Application, Washington, D.C. 20231

Type or Print Name: Carol Marstaller

Signature

**SYSTEM, METHOD AND APPARATUS FOR SECURE TRANSMISSION
OF CONFIDENTIAL INFORMATION**

CROSS REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of Assignee's U.S. Patent Application Serial No. 09/022,289, entitled "System, Method and Apparatus for Secure Transmission of Confidential Information", filed on February 11, 1998, and incorporates by reference Assignee's co-pending U.S. Patent Application Serial No. 08/845,938, entitled "Combined Mobile Telephone and Remote Control Terminal", filed on April 29, 1997.

BACKGROUND OF THE PRESENT INVENTION

Field of the Invention

The present invention relates generally to a system, method and apparatus for establishing a secure wireless communications link between two devices that minimizes the risk of third party interception of sensitive information, such as may be exchanged during communication initialization.

Background and Objects of the Present Invention

The evolution of wireless communication over the past century, since Guglielmo Marconi's 1897 demonstration of radio's ability to provide continuous contact with ships sailing the English Channel, has been remarkable. Since Marconi's discovery, new wireline and wireless communication methods, services and standards have been adopted by people throughout the world. This evolution has been accelerating, particularly over the least ten years, during which the mobile radio communications industry has grown by orders of magnitude, fueled by numerous technological advances that have made portable radio equipment smaller, cheaper and more reliable. The exponential growth of mobile telephony will continue to rise in the coming decades as well, as this

wireless network interacts with and eventually overtakes the existing wireline networks.

5 Cordless telephony has also been a part of the exponential rise in wireless telephony. Cordless telephones were originally aimed at providing economical, tetherless voice communications inside residences, i.e., using a short wireless link to replace the cord between a telephone base unit and its handset. Although early cordless phones were of marginal quality, with the introduction of improved
10 cordless phones in the 1980s sales dramatically increased. More recent advances, particularly in Europe, have extended the use domain of cordless phones outside of residences.

Another European revolution of cordless telephones is the digital enhanced cordless communications (DECT) standard,
15 which was optimized for use inside buildings. DECT controllers may hand off active calls from one base unit to another as the users move, and can page or ring handsets as a user walks through areas covered by different base units. As is understood in the art, however, the range of cordless
20 telephones is greatly limited compared to the more versatile cellular telephones, i.e., 0.3-30 or more kilometer range for cellular and less than 100 meters in cordless systems, and usually only up to tens of meters.

More recently, the worlds of cellular and cordless telephony have begun to converge with the introduction of cordless standards compatible with that of its cellular cousin. Accordingly, a mobile cellular user may utilize their cellular telephones within a cordless telephony system, thereby avoiding the need to purchase proprietary and typically non-compatible cordless telephones. Shown in FIGURE 1 is a private telephone system, generally referred to by the numeral 10, having at least one private base station 12 and a multiplicity of cellular phones 14 in communication therewith. When in a cordless mode a cellular user, e.g., at phone 14A, may communicate with another user within the private telephone system 10, e.g., another cordless-mode cellular phone 14B or a cordless phone 16, via the private base station 12 which serves as a relay.

One problem with the use of the cellular phones 14 within the private telephone system 10 is security. As discussed, original cordless telephones, e.g., phones 16 in FIGURE 1 were stand-alone consumer products that did not require any interoperability specifications. In other words, each cordless phone came with its own base station and needed to be compatible only with that base station. Billing, security and privacy concerns within such systems were

addressed by both preventing that cordless phone from
operating with any other base station and limiting the
transmission range of the cordless phones. With the
convergence of cordless and cellular technologies and the use
5 of interoperability specifications, however, the inherent
physical limitations of the cordless systems no longer serve
a security function. With cellular phones 14 being capable
of transmitting their signals over many kilometers, the use
of such phones within private telephone systems 10 raise
10 genuine security considerations.

As is understood in the art, cellular phone 14A may
communicate through the private base station 12 by use of
encryption keys or other such security protocol, whereby the
messages are encrypted and more difficult to decipher.
15 Accordingly, even though the communications from a cellular
user communicating within the private telephone system 10 may
extend well outside the outer reaches of the system 10, the
conversation or data exchanged is kept relatively confiden-
tial. Another problem, however, arises during communication
20 initialization over the radio interface which must occur
without encryption since no encryption keys have been
exchanged between the cellular user, e.g., of cellular
terminal 14A. The information is therefore being broadcast

across a wide range, including the keys, until encryption protocols are established. Accordingly, third parties may listen in on such pre-encryption transmissions and acquire sensitive information.

5 Various techniques may be employed to thwart such eavesdropping. A first approach is to use a wireline connection for the initial information exchange, whereby the cellular phone 14A must be electrically connected to the private base station to start the private communication.

10 This approach would, accordingly, require the definition of an electrical interface between the two components and limit the manufacturer's freedom to design attractive terminals since a standardized connector may increase the size and weight of the terminal. Further, such a definition may also

15 restrict further improvements of such phones 14, e.g., moving to lower voltage technologies for energy conservation and size deduction.

An alternative approach would be using Subscriber Identity Modules (SIMs) in both the private base station 10 and the respective cellular terminal 14, whereby the requisite identification information is readily established and the proper keys applied without transmitting them. In

20 addition to the added component costs, the use of two SIMs

in this manner also adds to the administrative costs of mobile network operators who must allocate unique SIM pairings between the private base stations 20 and respective cellular terminals 14. Furthermore, there is a risk that a
5 SIM meant for the cellular terminal 14 may instead be inserted into the private base station 12, further complicating this approach.

A third approach is to utilize the advantages of the radio interface, e.g., standardization. As discussed,
10 however, because radio waves propagate through walls and over large distances, this also poses a security risk which must be overcome.

In view of the disadvantages of each of the aforementioned approaches, it is clear that there is a need
15 for a simple and secure system and method for establishing a communications link between a first device, such as a cellular phone, and another device, such as a private base station.

It is, accordingly, an object of the present invention
20 to provide a system, method and apparatus for establishing such a simple and secure communications link, whereby at least a portion of a transmission, particularly one containing sensitive information, may be transmitted clearly

for proper reception while simultaneously minimizing the risk of interception.

It is a further object of the present invention to provide additional systems, methods and apparatuses that
5 securely transmit confidential or sensitive information for establishing a connection between a first and a second device that communicate via radio links, e.g., a lap-top computer and a peripheral device such as a printer.

It is another object of the present invention to provide
10 a secure wireless transmission link between any two devices, whether in the work-place or at home, e.g., a computer which receives an Internet command to turn on the heat in an apartment. After the establishment of the secure link, using the systems, methods and apparatuses of the present
15 invention, the two devices may then communicate via short- or long-range wireless radio links without the need for proprietary cables or other physical interconnection.

SUMMARY OF THE INVENTION

63222-0440-00250USP1

The present invention is directed to a system, method and apparatus for establishing a secure wireless radio communications link between two devices that minimizes the exposure of sensitive information to third party interception. The secure link is established by establishing an infrared link between the two devices for the exchange of sensitive information, such as encryption information. Subsequent communications would then have the benefit of encryption protection, establishing the secure wireless radio communications link.

A more complete appreciation of the present invention and the scope thereof can be obtained from the accompanying drawings which are briefly summarized below, the following detailed description of the presently-preferred embodiments of the invention, and the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGURE 1 is a schematic illustration of a private telephone system, including a private base station with cellular and cordless phones in communication therewith;

FIGURE 2 illustrates a dual-mode radiofrequency and infrared mobile station and private base station in accordance with the present invention;

FIGURE 3 illustrates various circuitry employed in the
5 dual-mode devices shown in FIGURE 2; and

FIGURE 4 illustrates a variety of devices that communicate with each other using the principles of the present invention.

10 **DETAILED DESCRIPTION OF THE PRESENTLY PREFERRED EXEMPLARY EMBODIMENTS**

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms
15 and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art.

20 The use of infrared (IR) transmissions between diverse electronic devices, e.g., between a television and a remote controller, are known, e.g., U.S. Patent Nos. 5,508,836,

5,588,009, 5,564,020, 5,617,236 and 5,446,783 each describe various IR-electronic interconnections. U.S. Patent No. 5,636,264 similarly describes an IR interface between a phone handset and a computer. Although generally describing the
5 usage of IR in these contexts, the references fail to discuss the aforementioned security problems inherent in wireless communications nor the proposed solution set forth in the present invention, described in more detail hereinafter.

Shown in FIGURE 2 is a dual mode mobile station 20 in
10 communication with a dual mode private base station 21. As discussed, mobile station 20 communicates with the private base station 21 via an RF transmission, which has an effective range of hundreds of meters, and via a more limited, "cordless" communications mode having a much
15 shorter, contained range. As is understood in the art, the RF transmission mode is via the respective antennae 20A and 21A of the mobile station 20 and private base station 21, respectively, the signals being transceived in a conventional manner.

20 Also shown in FIGURE 2 are IR transceiver interfaces 20B and 21B on the mobile station 20 and private base station 21, respectively. Each interface preferably includes a photodetector 22 for receiving IR signals and an IR signal

emitter 23 for transmitting such IR signals. It should be understood that the position of the interfaces 20B and 21B on the respective bodies of the mobile station 20 and the private base station 21 are arbitrary, provided the
5 respective IR signals to and from the interfaces 20B and 21B are not blocked, e.g., by the palm or fingers of the phone user. In other words, ergonomic considerations may dictate particular placements for the interfaces, as is understood in the art.

10 With further reference to FIGURE 2, one of the practical utilizations of the dual-mode mobile station 20 is now illustrated. In particular, when the dual-mode mobile station 20 comes within the more limited range of the private base station 21, e.g., in the same or an adjacent room, the
15 subscriber may wish to transfer control from the cellular provider to the private system, e.g., to save money on the cheaper wireline phone rates through the private system to the Public Switched Telephone Network (PSTN). For example, through the PSTN 24, the mobile station 20 can communicate
20 with remote wireline phones 25 and remote cellular phones 26 via a base transceiver system 27 (shown for simplicity as a base transceiver station tower).

With reference now to FIGURE 3 of the drawings, there is illustrated a portion of the mobile station 20 (in FIGURE 2), particularly, the IR transceiver interface 20B and various circuitry within the mobile station 20 for handling the IR signals. An IR receiver or photodetector 30 receives the IR signals, such as from the private base station 21, and passes the signals to a decoder 31, which converts the infrared information within the IR signal to electrical information, e.g., digital pulses. The converted information is then forwarded to a controller 32, which controls the flow of the electrical information (pulses). A signal conversion device 33 receives the aforesaid electrical information flow and groups the incoming pulses into a unit size (frame) pursuant to a known signal format. The controller 32 may be a UART or other like controller, as is understood in the art.

The incoming signal, now translated, is sent to a processor 34, which implements the command(s) set forth in the signal, e.g., forward the incoming signal to another phone such as mobile station 14B (in FIGURE 1) across the RF communications link. Similarly, the processor 34, in response to one or more commands, may send a message across the IR communications link by first forwarding the message to the signal conversion device 33, which converts the

structured message into the aforesaid electrical information or pulses, which the controller 32 sends to an encoder 35. The electrical pulses are there converted to IR radiation signals which are then transmitted by an IR transmitter 36, e.g., light emitting diodes, releasing the IR signal.

It should, of course, be understood that the circuitry shown in FIGURE 3 is preferably also incorporated within the private base station 21 so that a wireless IR dialogue may be established with the mobile station 20.

As discussed, the effective range of the IR signal so emitted is limited, e.g., on the order of several dozens of meters. With obstacles like walls, floors and ceilings, the effective range is even further reduced, as is encountered by consumers with products such as television remotes. Accordingly, IR signals provide an excellent way to exchange confidential information wirelessly, effectively limiting communications to a point-to-point conversation, albeit preferably temporarily until the security protocols are safely established. Eavesdropping, although still possible, is thwarted by such range restrictions since other security measures, e.g., building control, may be employed in conjunction to provide almost any level of interception prevention.

Since various encryption methods are available to make a wireless conversation almost impervious to code-breakers, wireless communications between a user of the dual-mode phone 20 (in FIGURES 2 and 3) preferably switches to the RF communications mode to utilize the enhanced security advantages of encryption to prevent deciphering. Wireless RF communications, however, even with encryption, are easily intercepted by a distant eavesdropper. Although encryption data may thwart the eavesdropper's deciphering the intercepted coded message, the caller and recipient must first establish the secure transmission through the exchange of encryption keys over a non-encrypted wireless communication, which the eavesdropper can monitor, easily decipher the pertinent keys and then decipher the supposedly secure encrypted transmissions.

The system, method and apparatus of the present invention provide an improved, more secure way to preserve the confidentiality of wirelessly transmitted information by restricting exposure of the encryption keys and any other confidential information through use of the aforementioned IR transmissions.

In one embodiment of the present invention the subscriber of mobile station 20 when sufficiently close to

the private telephone system, e.g., near the private base station 21, activates the mobile station 20 to emit an IR signal, e.g., via IR transmitter 36. Alternatively, the mobile station 20 may activate IR signaling capability automatically in advance of transceiving any security-related data. In a preferred embodiment of the present invention, the mobile station utilizes conventional radiofrequencies for all non-security-related transmissions, e.g., when initiating communications with the private base station 21 such as a cordless telephone base station and after the exchange of encryption or other such security data. Upon reaching the aforementioned security data or protocols in the transmission, the mobile station 20 then switches over to the aforementioned IR signaling using the IR transmitter 36.

It should be understood, that the RF-to-IR switchover may occur early in the transmission, e.g., in the initial communications attempts, or later during the transmission, so long as any secured portions of the signal are transmitted via IR transmissions.

In either event, the private base station 21 detects the IR signal transmission from the mobile station 20, via the aforementioned photodetector 30 in the station 21, processes the incoming IR signal, and responds with an IR response

signal, which preferably includes an encryption key. It should be understood that one or more encryption keys may be inserted into the response signal by an encryption device 37 in communication with the processor 34. Upon the secure receipt of the encryption key(s) from the private base station 21 via IR transmission, the mobile station 20 may then safely begin/resume wireless RF communications, which are now encrypted pursuant to the embedded encryption key(s). The subscriber is then able to move more freely throughout the building, all the while taking advantage of the inexpensive wireline communications link through the PSTN 24, as discussed hereinbefore.

In another embodiment of the present invention, the private base station 21 may periodically emit an IR signal, which the mobile station 20 may intercept, if close enough. In effect, the private base station may perform an IR poll to establish the preliminary IR linkage to exchange security information, such as the aforescribed encryption keys. For example, upon detection (in photodetector 30), the mobile station 20 may (like the private base station 21 in the previous embodiment) also respond with an IR response signal, which may include encryption key(s) for governing the subsequent RF transmissions with the private base station 21,

thereby providing a procedure for periodic or random security measures.

In still another embodiment of the present invention, the more secure IR communications link may be employed by the subscriber of the mobile station 20 or an administrator of the private telephone system to transfer other, non-initialization-related information. For example, if particularly sensitive information needs to be transmitted during an RF communication, the mobile station 20 and private base station 21 may switch to the more private IR communications mode and resume the RF mode transmissions after the sensitive information has been transferred. It should also be understood that the mobile station 20 and private base station 21 may automatically revert to the IR communication mode while in range of each other and only switch over when the IR transmissions begin to deteriorate.

Although one preferred embodiment of the present invention utilizes the principles of the present invention in the context of mobile telephony, it should be understood that the scope of the present invention, as set forth in the claims hereinbelow, covers a variety of dual-mode wireless interconnections using an infrared mode for security purposes.

With reference now to FIGURE 4, there is illustrated a further embodiment of the present invention in which a first device, such as a mobile phone, a headset on a user or a computer, communicates with at least one of a large number of other devices, such as set forth in detail in Assignee's
5 pending patent application entitled "Combined Mobile Telephone and Remote Control Terminal", U.S. Patent Application Serial No. 08/845,938, filed April 29, 1997, incorporated herein in its entirety by reference. It should
10 be understood that although all of the various devices depicted in FIGURE 4 may be able to communicate with each other, certain pairings may not be utilized (at present). For example, a printer 50 (receiving commands from a personal computer or PC 48) need not communicate with a television 68,
15 although the television 68 could transmit an image for printing at the printer 50. The printer 50, however, could well forward a printing completion message (or out-of-paper or error message) to the PC 48 (using the security measures of the instant application or not).

20 Recent initiatives, such as the Bluetooth Mobile Communications Initiative, are promoting the increase in interoperability of the various electrical, electronic and mechanical devices utilized in the work place and at home.

5 A number of the various devices capable of using the
Bluetooth or other like technology are illustrated in FIGURE
4, including a home base station 40 which is linked to a
conventional Public Switched Telephone Network (PSTN) 42,
10 converting the wireless rf and infrared signals received from
other devices, such as the dual-mode phones 26 (shown in
FIGURE 2), a wireless headset/hands-free unit 44 or other
cordless device 46. The desk-top or lap-top PC 48 may also
interact with a number of additional peripheral devices,
15 e.g., printer/plotter/projector 50, a facsimile 52, a pager
54, a data organizer 56 or other such personal, hand-held
organizer device (enabling the download of sensitive
information both to and from the organizer 56 and
synchronization with data stored in the PC 48, another PC 57
20 or an electronic data terminal 58), a scanner 60, microphone
62, a PC card 64 and numerous other such peripherals,
generally designated by the reference numeral 66. Of
course, the principles of the present invention are also
applicable in the mobile station 26 and a SIM card 26A, such
as the one associated therewith, or a SIM card 67 separate
from mobile station 26 as illustrated in FIGURE 4.

In the home, numerous other household devices may be
equipped with the dual-mode functionality such as set forth

in the present invention. For example, the PC 48 may intercommunicate with the television 68, a radio 70, a stereo 72 or peripheral attached thereto, or a VCR or other video player 74 (tape or disk). Other interconnected devices in the home include a light device (lamp) 76, a dimmer switch 78, a thermostat 80 to control heating/cooling of a domicile, a door device 82 such as a garage door, a refrigerator/freezer 84, a cooking device 85 (microwave, gas, etc.), a washer/dryer 86, an answering machine 88 and an alarm device 90. Additional devices that may include the inventive techniques of the present invention include a car alarm 92 (with a car lock feature), which to operate in infrared mode must be in close proximity, preferably also in line-of-sight, and other external alarm devices which may be stationary.

Utilizing the principles of the present invention, secure communications may be established, via the infrared and wireless links, enabling a user, e.g., through voice or keyed-entry commands entered into a handheld or wrist (watch) communication device, generally designated by the reference numeral 94, to open their garage door 82, exit and lock their car, disarm their home alarm devices 90, and enter their domicile which has been heated/cooled by a prior remote

command to the thermostat 80 (relayed wirelessly by the home PC 48).

It should be understood that although the plethora of wirelessly interconnected devices, such as specified pursuant to the Bluetooth initiative, may utilize low-cost, short-range radio links instead of the expensive, cumbersome and proprietary cabling now required, the need for securing these rf transmissions, which may range for a hundred meters or more, is critical since an unauthorized user could easily eavesdrop, intercept and decrypt these communications, thereby gaining access to the personal domain and effects of a user. The initial, more secured infrared transmissions of the present invention, requiring close proximity, more line-of-sight security data exchanges, provide the requisite level of protection necessary in these open-to-tampering systems.

Frequency spectrums available for these private applications are, at present, rather limited. In the United States, for instance, bands at 900 MHZ, 2.4 GHz and 5.7 GHz are currently unlicensed and may be used freely, provided the transmission (TX) power levels are low or spreading is applied. The Bluetooth initiative is scheduled to operate at the globally-available 2.45 GHz Industrial, Scientific, Medical (ISM) 'free band', allowing international travelers

to employ Bluetooth-enabled equipment worldwide. It is understood to those skilled in the art that in an effort to avoid interference, spreading should be applied either by Frequency Hopping (FH) or direct-sequence (DS) spread spectrum. The 2.45 GHz ISM band may be used for a variety of devices and constitutes a band ranging from about 2.4 GHz to about 2.483 GHz, as described in Assignee's co-pending patent application entitled "Method and Apparatus for Tracking a Mobile Phone". As discussed in said patent application, describing frequencies in a phone tracking system, in an effort to avoid sharp filters to fulfill out-of-band emission requirements, the applied radio band is preferably placed away from the ISM band edges. Known interference areas, e.g., from 2.435 GHz to 2.465 GHz in which microwave ovens operate, are preferably avoided as well. Frequency Shift Keying (FSK) can be used to map the user code on the rf carrier. In such an FSK modulation technique, a bit representing 'one' is mapped to the frequency $rf + Df$, and a bit representing 'zero' is mapped to the frequency $rf - Df$ (or vice versa) where rf is the carrier frequency and Df is the frequency deviation, which should be large enough to combat the frequency offset between the transmitter and the receiver. For example, if inaccurate

frequency references (with an accuracy of about 50 parts per million) are used, the worst-case frequency offset can reach up to 240 KHz. In order to receive the burst in such a case, the frequency duration D_f should be greater than 240 KHz.

5 It should be understood that although GSM technology is presently preferred, the principles of the present invention may also be employed in other Time Division Multiple Access (TDMA), Personal Digital Cellular (PDC) and presently developed (and future) third generation systems and
10 equipment. Consequently, the various frequencies used by these and other systems, e.g., 800, 900, 1500, 1800, 1900, 2000 and 2100 MHz bands, may also be employed in the system, method and apparatus of the present invention.

15 The previous description is of preferred embodiments for implementing the invention, and the scope of the invention should not necessarily be limited by this description. The scope of the present invention is instead defined by the following claims.